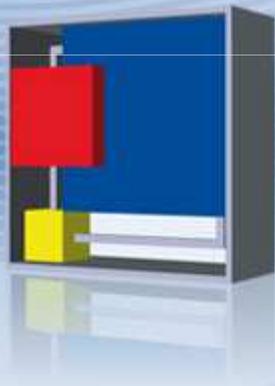


# Cloud Computing - Infonuagique

## Une prestation comme une autre ?



ALAIN BENSOUSSAN  
LE DROIT DES TECHNOLOGIES AVANCÉES

Eric Barbry  
Avocat à la Cour  
Directeur du département « droit du numérique »

# PLAN

1. Présentation synthétique
2. Les risques « amont »
3. Les risques « pendant »
4. Les risques « après »



# 1. Présentation synthétique

1.1. Avantages

1.2. Types

1.3. Impacts



# Tout ce dont vous avez toujours rêvé...

Des serveurs autant que de besoin et modulable

Adaptation à la montée en charge des besoins client

Une capacité de stockage illimitée

Une bande passante de rêve

Des interface web sympas

Un service a la demande

Une agrégation de ressources

Un travail « any where »

Un haut débit et networking

Monitoring global et complet

Un paiement à la consommation

Facilite les mises à jour

Dernier cri technologique

**Le cloud c'est top**



# On devrait dire ... « Les » clouds

- Cloud public : externe à l'entreprise généralement mutualisé
- Cloud privé (privatif) : réservé à un utilisateur ou sous son contrôle exclusif (entreprise + client + fournisseurs, ...)
- Cloud communautaire : accessible à une communauté d'intérêt généralement « administré » par un membre
- Cloud hybride : Combinaison de cloud privilégiant l'interopérabilité



# 3 modèles pour un seul Cloud

Couche applicative, en Saas

Couche plateforme, en Paas

Couche infrastructures, en Iaas

+ Xaas (Anything or everything as a service)

+Vaas (vidéo as a service)

+ PRaas (Plan de reprise as a service)

And so and so



# Le cloud n'est pas une prestation de « sous-traitance »

- Une prestation de service, certes mais
- Une virtualisation
- Une dématérialisation
- Une nouvelle organisation du travail



# Le cloud ça change tout et ça change rien

Rien n'est chez moi

Mais tout est à moi

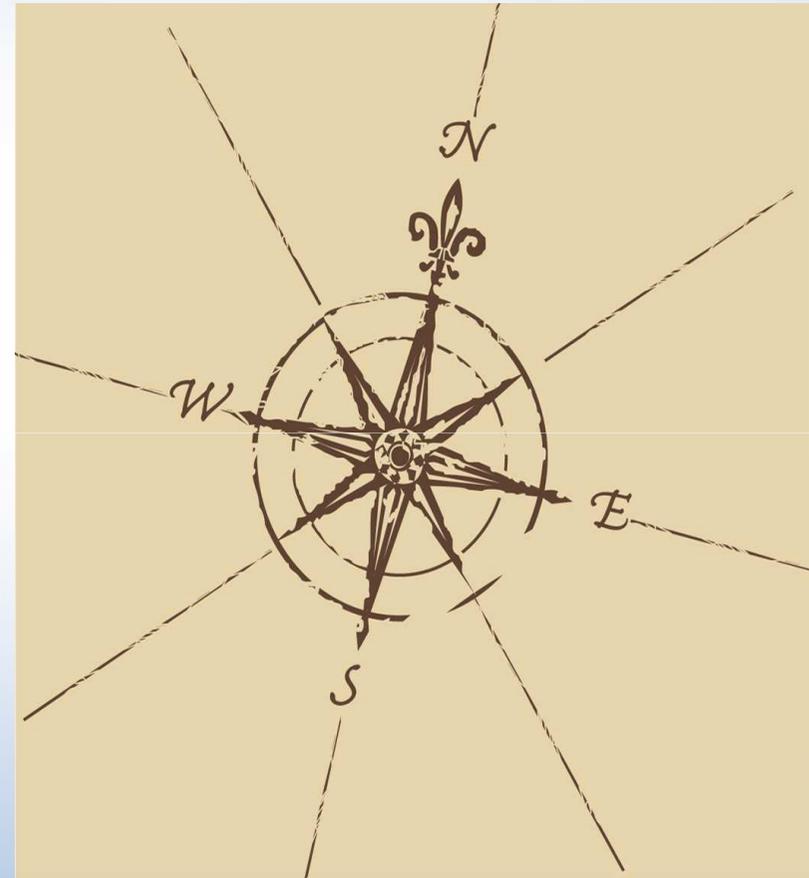


## 2. Risques amont

2.1. Faisabilité légale

2.2. Faisabilité impact

2.3. Faisabilité sociale



# Toutes n'est pas Cloudisable... ou alors sous fortes contraintes

- Données de santé
  - Dispositions spécifiques légales
- Données bancaires
  - Dispositions spécifiques légales
- Opérateurs d'infrastructure vitale
- AA soumis au RGS

- Acteurs soumis au secret défense
  - Instruction générale inter ministérielle sur la protection du secret de la défense nationale
- Plate-forme agréées
  - Ex : Jeux d'argent en ligne
- Entreprises certifiées

# Maîtrise du risque

**ETUDE DE FAISABILITE**

**PRE REQUIS**

**REFERENTIEL DOCUMENTAIRE  
CODE DU DSI**

# Et même si c'est faisable juridiquement , Attention à l'impact

Engagements contractuels

Réalité technique

Réalité organisationnelle

Réalité commerciale



**Etude  
d'impact**



# Mais est-ce bien légal ?

## Un premier problème majeur...

### Sécurité des données

« Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Des décrets, pris après avis de la Commission nationale de l'informatique et des libertés, peuvent fixer les prescriptions techniques auxquelles doivent se conformer les traitements mentionnés au 2° et au 6° du II de l'article 8. » - Art. 34 I&L

### Sécurité et sous-traitance

« Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement.

Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi.

Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en oeuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures.

Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement.

# Ca pourrait bien s'aggraver...

« Le responsable du traitement met en œuvre toutes les mesures adéquates, au regard de la nature des données et des risques présentés par le traitement, pour assurer la sécurité des données et en particulier protéger les données à caractère personnel traitées contre **toute violation entraînant accidentellement ou de manière illicite la destruction, le stockage, le traitement ou l'accès non autorisé ou illicite.**

En cas de violation du traitement de données à caractère personnel, **le responsable de traitement avertit sans délai le correspondant "informatique et libertés" ou, en l'absence de celui-ci, la Commission nationale de l'informatique et des libertés.** Le responsable du traitement, avec le concours du correspondant "informatique et libertés", **prend immédiatement les mesures nécessaires** pour permettre le rétablissement de la protection de l'intégrité et de la confidentialité des données. **Le correspondant "informatique et libertés" en informe la Commission nationale de l'informatique et des libertés.** Si la violation a affecté les données à caractère personnel d'une ou de plusieurs personnes physiques, **le responsable du traitement en informe également ces personnes**, sauf si ce traitement a été autorisé en application de l'article 26. Le contenu, la forme et les modalités de cette information sont déterminés par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés. Un inventaire des atteintes aux traitements de données à caractère personnel est tenu à jour par le correspondant "informatique et libertés"

Des décrets, (...)

# Mais est-ce bien légal ?

## Un deuxième problème majeur...

### Flux de données

La règle : Interdiction sauf

Le « représentant » en France

### Les exceptions

- EU
- Pays protection adéquate
- Safe Harbor
- Convention
- Exceptions limitées

# Le risque social

« Le comité d'entreprise est informé et consulté, préalablement à tout **projet important d'introduction de nouvelles technologies**, lorsque celles-ci sont susceptibles d'avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail.

Les membres du comité reçoivent, un mois avant la réunion, des éléments d'information sur ces projets et leurs conséquences sur chacun des sujets mentionnés au premier alinéa. »

Article L2323-13 C du travail

## 3. Risque « pendant »

3.1. Localisation juridique

3.2. Accessibilité

3.3. Sécurité

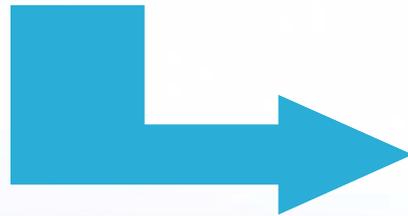
3.4. Risque financier

3.5. Gestion de la preuve



# Quel droit applicable ?

Le droit du contrat



Simple = Clause

Le droit des données

**Risque : Accès aux données**  
Droit local

# Accessibilité

- Le « bonheur » n'existe pas ☹
- Les risques d'inaccessibilité existent
- La maîtrise du rétablissement
  - Insuffisant
- Les pénalités
  - Une incitation complémentaire
    - Le plafond est un vrai problème
    - Les dommages directs aussi



# La sécurité au cœur du Cloud

Besoin de réactivité

Risque sur données

Plus de cibles ?

Qui est responsable ?

Risque sur les flux

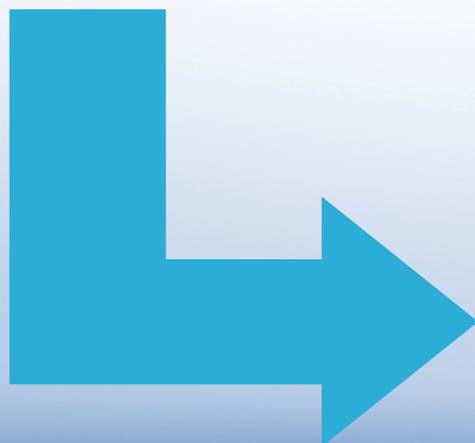
# Gestion de la preuve

- La preuve aussi est dans le nuage
- La preuve est de chaque instant
  - Contentieux commercial
  - Contentieux prud'hommal
- Obligation légales de conservation des données
  - Ex : Logs de connexion
- Exigence de disposition contractuelle spécifique



# Risque financier

Difficulté d'appréciation des besoins réels  
Complexité des paramètres de facturation  
Perte de visibilité sur le coût des services  
Difficultés pour benchmarker le prix



## Clause spécifique

- Estimation
- Review et audit financier
- Benchmark (à la charge du prestataire)



# Le cloud ça change tout et ça change rien (en droit)

Clauses classiques

Nécessaires mais pas  
suffisantes

Nouvelles clauses

Nouvelle organisation  
contractuelle



# Le risque du pluriel

Au niveau des prestataires

Au niveau des utilisateurs  
(Cloud privé ou communautaire)



**Contrat de  
gouvernance**



**Convention  
Cloud Computing**

## 4. Risque « aval »

4.1 Fin de contrat

4.2 Disparition



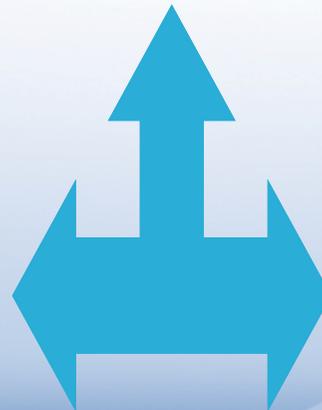
# Le risque de fin de contrat

Je n'ai plus rien...

Mais tout est à moi ...

Je veux tout récupérer, tout de suite et sans risque

**Reversibilité  
sortante**



**Reversibilité  
entrante**

# Le pire... la disparition inattendue du prestataire Cloud

Les grands classiques...

Assurez vous !  
Garantissez vous !



# Cinq conseils

- A1 – Etude amont
  - de faisabilité légale
  - d'impact (dont le juridique)
- A2 – Pre-requis juridiques
- A3 – Clauses spéciales Cloud Computing
- A4 – Contract management
- A5 – Audit assurance



# Pour en savoir plus

- Travaux de ENISA « benefits, risks and recommendations for information security Cloud Computing » - 2009

<http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment>

- « L'informatique dématérialisée en nuages » Daniel Guinier - « Expertise des systèmes d'information » - Oct 2010

- Mémoire « Cloud computing, SSI et investigations judiciaires, Hervé Putigny, 2010

- Livre blanc du Syntec numérique

<http://www.syntec-numerique.fr/actualites/liste-actualites/publication-du-livre-blanc-cloud-computing-de-syntec-informatique>



[Retour au Figaro.fr](#) [Tous les blogs du Figaro](#)

**DROIT DES TECHNOLOGIES AVANCÉES**



**FIGARO**  
BLOG EXPERT

Alain Bensoussan  
Eric Barbry

## Le « cloud computing », quand le droit aussi est dans les nuages

[S'abonner au flux de ce blog](#)

Par [Eric Barbry](#) le 19 mai 2010 14h54 | [Un commentaire](#)

Le Cloud Computing est un sujet d'actualité. Toutes les entreprises s'interrogent aujourd'hui sur cette nouvelle offre de service. Après le SaaS (Software as a Service) et le PaaS (Platforms as a Service), le Cloud Computing (autrement appelée « informatique dans les nuages ») constitue une nouvelle forme d'externalisation.

Le Cloud Computing repose sur une offre de service dynamique et modulable qui elle-même, repose sur le fait que l'information est stockée et accessible dans n'importe quel « point » du nuage et non nécessairement sur un serveur parfaitement identifié par l'entreprise. A la différence des solutions précédentes d'externalisation, le Cloud induit une « dispersion » de l'information.

De fait, le Cloud computing de part cette spécificité, pose aujourd'hui des questions nouvelles à celles des entreprises -nombreuses-, qui s'interrogent sur le fait d'opter pour ce type de service.

La première question qui se pose, est celle de la légalité de l'opération elle-même. Non pas que le Cloud soit illégal en soit mais il n'est pas certain que toutes les données soient « cloudables ». Certaines données font en effet l'objet de protections particulières et il n'est pas certain qu'elles puissent être disséminées et traitées par un tiers, sauf à prendre des précautions particulières. On peut ainsi s'interroger sur le caractère « cloudable » ou non, des données bancaires ou des données de santé, par exemple.

Une fois traitée cette question primordiale, une autre question ne manquera pas de se poser : Quel contrat conclure et avec qui ?

Le contrat cloud de ce point de vue, n'est pas un contrat comme un autre. Certes, il s'agit d'un contrat d'externalisation et en ce sens, il comportera toutes les dispositions relatives à ce type de prestations, mais là encore, la spécificité du cloud computing impose une rédaction adaptée de chacune de ces clauses.

A titre d'exemple, la clause de « sécurité » devra nécessairement être renforcée du fait des risques particuliers liés au fait que la maîtrise technique repose essentiellement sur le prestataire et qu'il conviendra de traiter très spécifiquement les conditions d'accès aux éléments de l'entreprise. Les clauses de « garantie » elles aussi devront être renforcées car dès lors que toute l'entreprise et ses données seront externalisées, la moindre difficulté en terme d'accès aux applications ou aux données cessera l'exercice d'activité du client ou un fonctionnement en mode pour le

A propos de ce blog

Des idées nouvelles aux usages nouveaux... quelles problématiques juridiques ? - web 2.0, web 3.0, identité numérique, scanner corporel, réalité augmentée, avatars et pseudo, ... Décodage et éclairage par deux avocats, [Alain Bensoussan](#) et [Eric Barbry](#).



Rechercher

Nuage de tags

[2010](#) [accès internet](#) [accès à internet](#) [aka-aki](#) [Alain Bensoussan](#) [Ariel](#) [atelier sur le droit à l'oubli numérique](#) [Atteinte à la personne humaine](#) [atteinte à la vie privée](#) [authenticité](#) [charte des droits fondamentaux de l'union européenne](#) [Cnil](#) [droit à la vie privée](#) [Eric Barbry](#) [Facebook](#) [identité numérique](#) [liberté d'expression](#) [loi Informatique et libertés](#) [réseaux sociaux](#) [vie privée](#)

Liens

# Contact

- ALAIN BENSOUSSAN AVOCATS

29 rue du colonel Pierre Avia Paris 15<sup>e</sup>



Tél. : 33 1 41 33 35 35

Fax : 33 1 41 33 35 36



[paris@alain-bensoussan.com](mailto:paris@alain-bensoussan.com)

- Eric Barbry



L.D. : 33 1 41 33 35 27

Mob. : 33 6 13 28 91 28



[eric-barbry@alain-bensoussan.com](mailto:eric-barbry@alain-bensoussan.com)

**MERCI**

